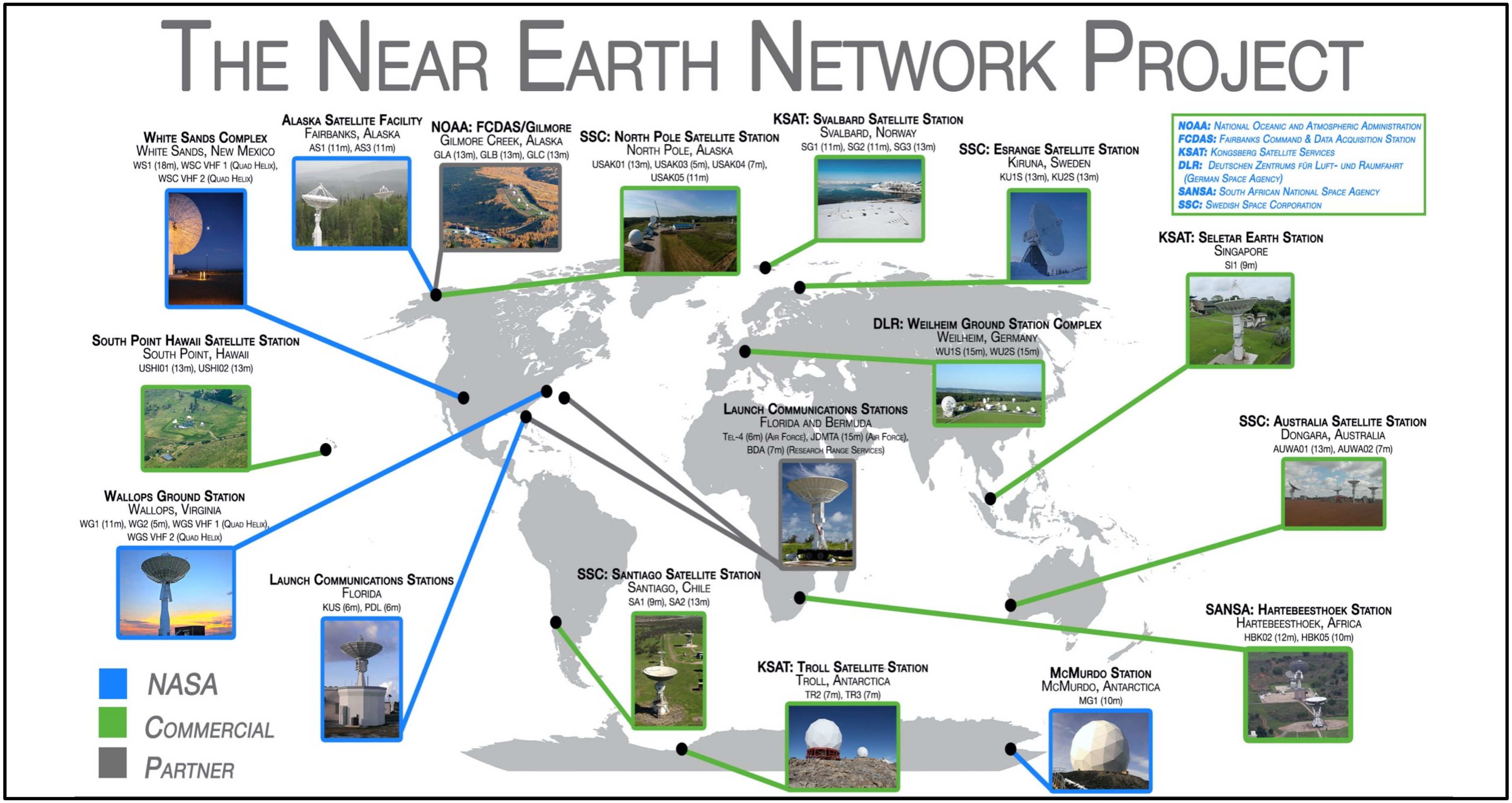
NANOG 84

Pwned in Space

Paul Coggin
Cyber SME
Nou Systems, Inc

Example Ground Systems Network
NASA



The Near Earth Network Project

White Sands Complex
White Sands, New Mexico
WS1 (18m), WSC VHF 1 (Quad Helix), WSC VHF 2 (Quad Helix)

Alaska Satellite Facility
Fairbanks, Alaska
AS1 (11m), AS3 (11m)

NOAA: FCDAS/Gilmore
Gilmore Creek, Alaska
GLA (13m), GLB (13m), GLC (13m)

SSC: North Pole Satellite Station
North Pole, Alaska
USAK01 (13m), USAK03 (5m), USAK04 (7m), USAK05 (11m)

KSAT: Svalbard Satellite Station
Svalbard, Norway
SG1 (11m), SG2 (11m), SG3 (13m)

SSC: Esrange Satellite Station
Kiruna, Sweden
KU1S (13m), KU2S (13m)

NOAA: National Oceanic and Atmospheric Administration
FCDAS: Fairbanks Command & Data Acquisition Station
KSAT: Kongsberg Satellite Services
DLR: Deutschen Zentrums für Luft- und Raumfahrt (German Space Agency)
SANSA: South African National Space Agency
SSC: Swedish Space Corporation

KSAT: Seletar Earth Station
Singapore
SI1 (9m)

South Point Hawaii Satellite Station
South Point, Hawaii
USHI01 (13m), USHI02 (13m)

DLR: Weilheim Ground Station Complex
Weilheim, Germany
WU1S (15m), WU2S (15m)

Launch Communications Stations
Florida and Bermuda
Tel-4 (6m) (Air Force), JDMTA (15m) (Air Force), BDA (7m) (Research Range Services)

SSC: Australia Satellite Station
Dongara, Australia
AUWA01 (13m), AUWA02 (7m)

Wallops Ground Station
Wallops, Virginia
WG1 (11m), WG2 (5m), WGS VHF 1 (Quad Helix), WGS VHF 2 (Quad Helix)

Launch Communications Stations
Florida
KUS (6m), PDL (6m)

SSC: Santiago Satellite Station
Santiago, Chile
SA1 (9m), SA2 (13m)

SANSA: Hartebeesthoek Station
Hartebeesthoek, Africa
HBK02 (12m), HBK05 (10m)

KSAT: Troll Satellite Station
Troll, Antarctica
TR2 (7m), TR3 (7m)

McMurdo Station
McMurdo, Antarctica
MG1 (10m)

🟦 NASA
🟩 Commercial
⬛ Partner

Source: https://www.nasa.gov/sites/default/files/thumbnails/image/high_res_nen_working_poster.jpg

Ground Station as a Service (GaaS)

nousystems inc

Amazon AWS, MS Azure, Google offer GaaS

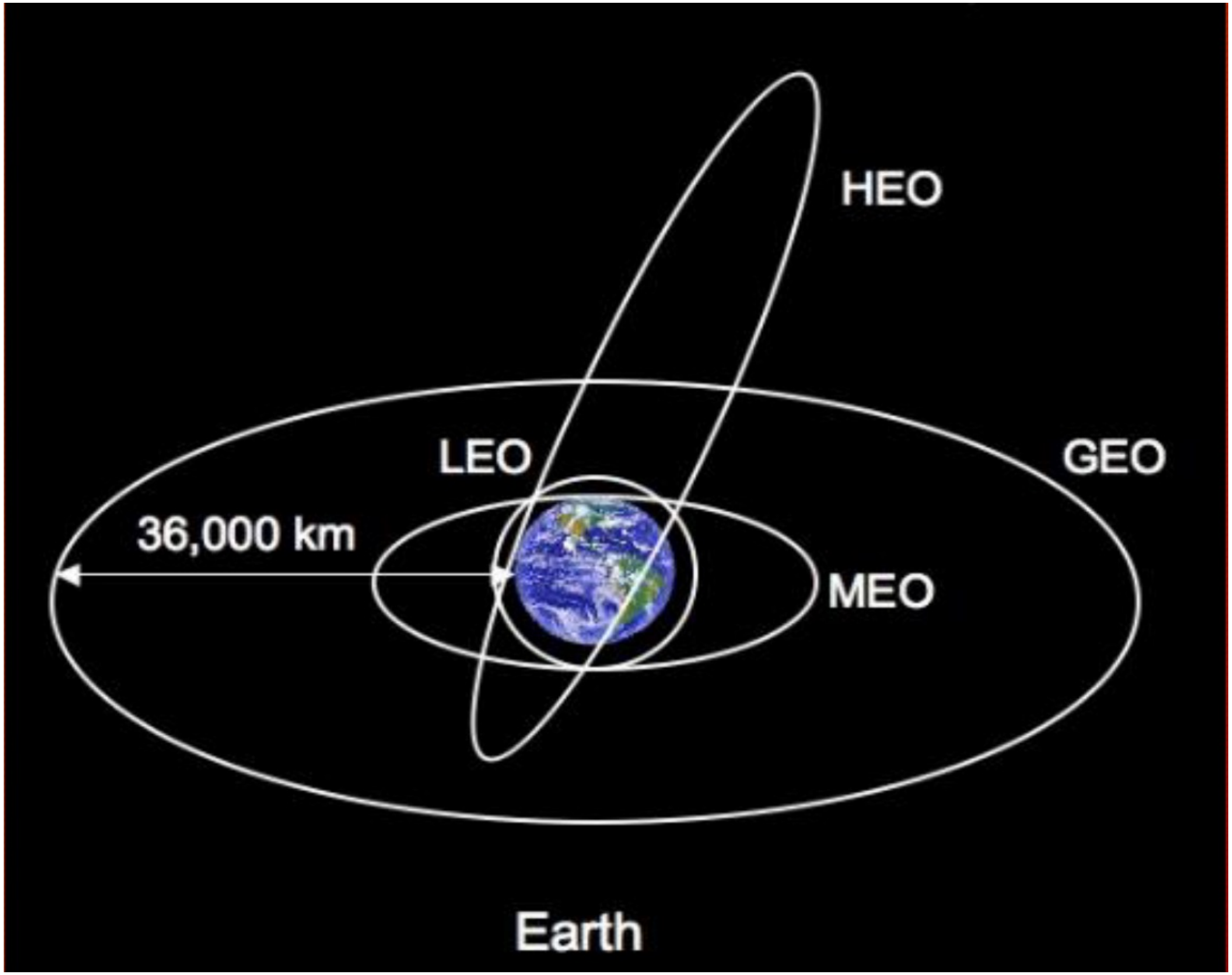
Satellite Orbits

LEO
- 160 – 2,000 km

HEO
- 16,000 x 133,000 km

MEO
- 2,000 – 35,786 km

GEO
- 35,786 km



Source: NASA , https://www.nasa.gov/sites/default/files/atoms/files/66_cost_effects_of_destination_on_space_mission_cost_v6.pdf

Space Threat Analysis

According to the Federation of American Scientists, there are five main categories of threat for spacecraft:

1. **Deception: Target reports incorrect information.**
2. **Disruption: Target's capability temporarily degraded.**
3. **Denial: Target's capability temporarily disabled.**
4. **Degradation: Target's capability degraded irreparably.**
5. **Destruction: Complete loss of target spacecraft.**

Sources: https://www.spacesymposium.org/wp-content/uploads/2017/10/Hanlon-Edward_Survivability-Analysis-of-a-Small-Satellite-Constellation_1.pdf , https://spp.fas.org/eprint/article05.html

Space System Cybersecurity Threats

nousystems inc

- Jamming
- Malware
- Spoofing
- Control Payload
- Control TT&C
- Replay
- Hacking
- Hijacking
- Eavesdropping

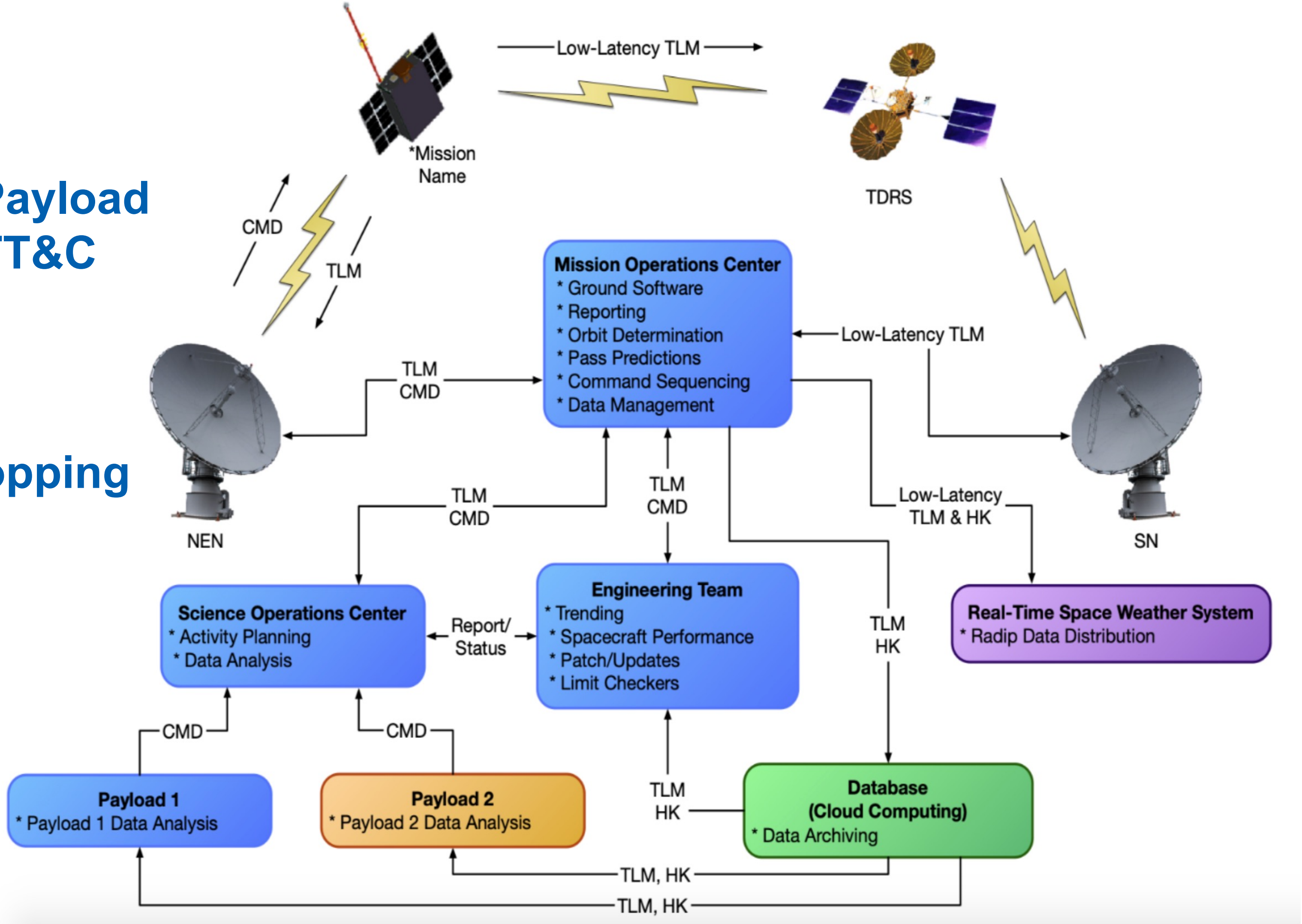
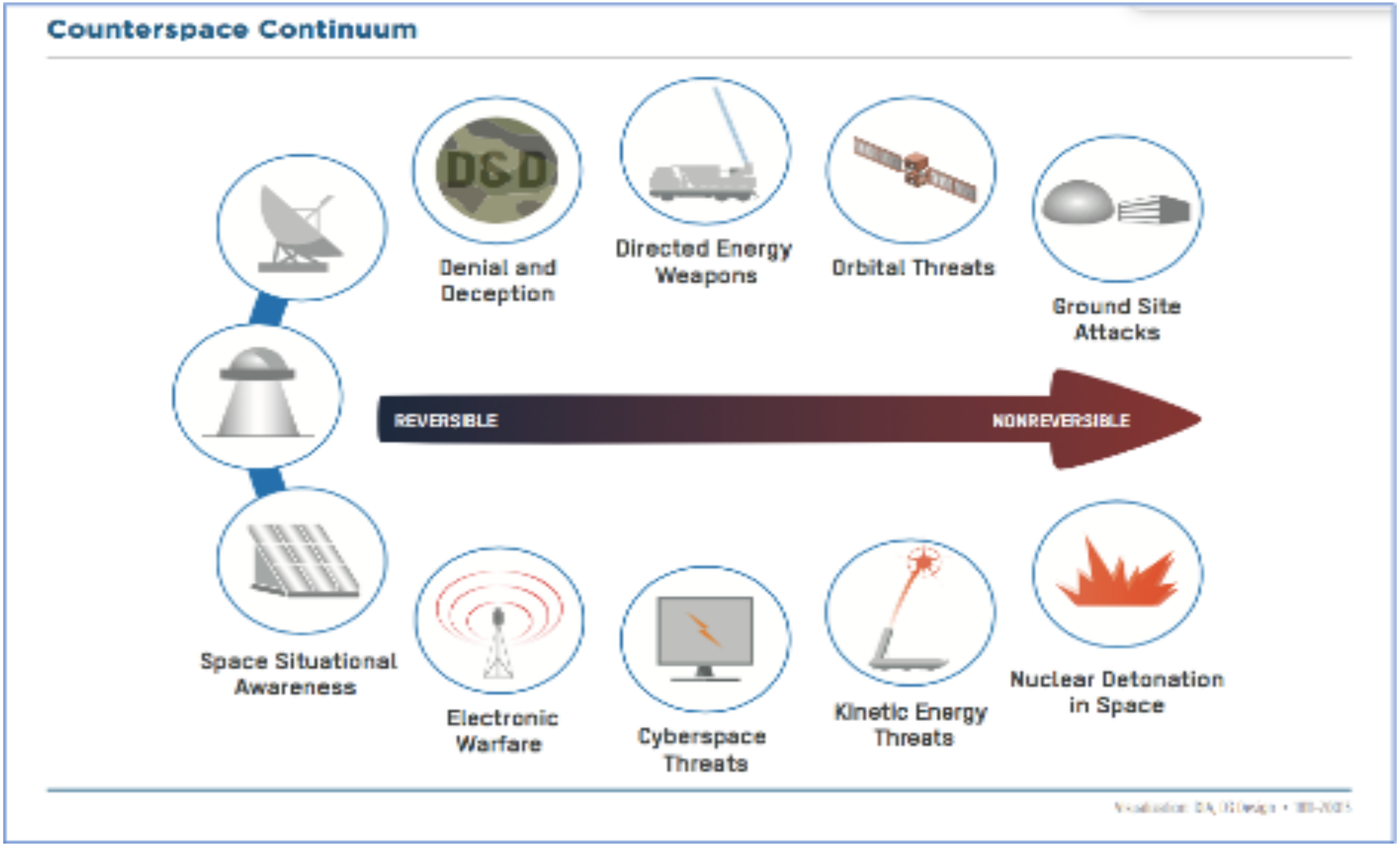


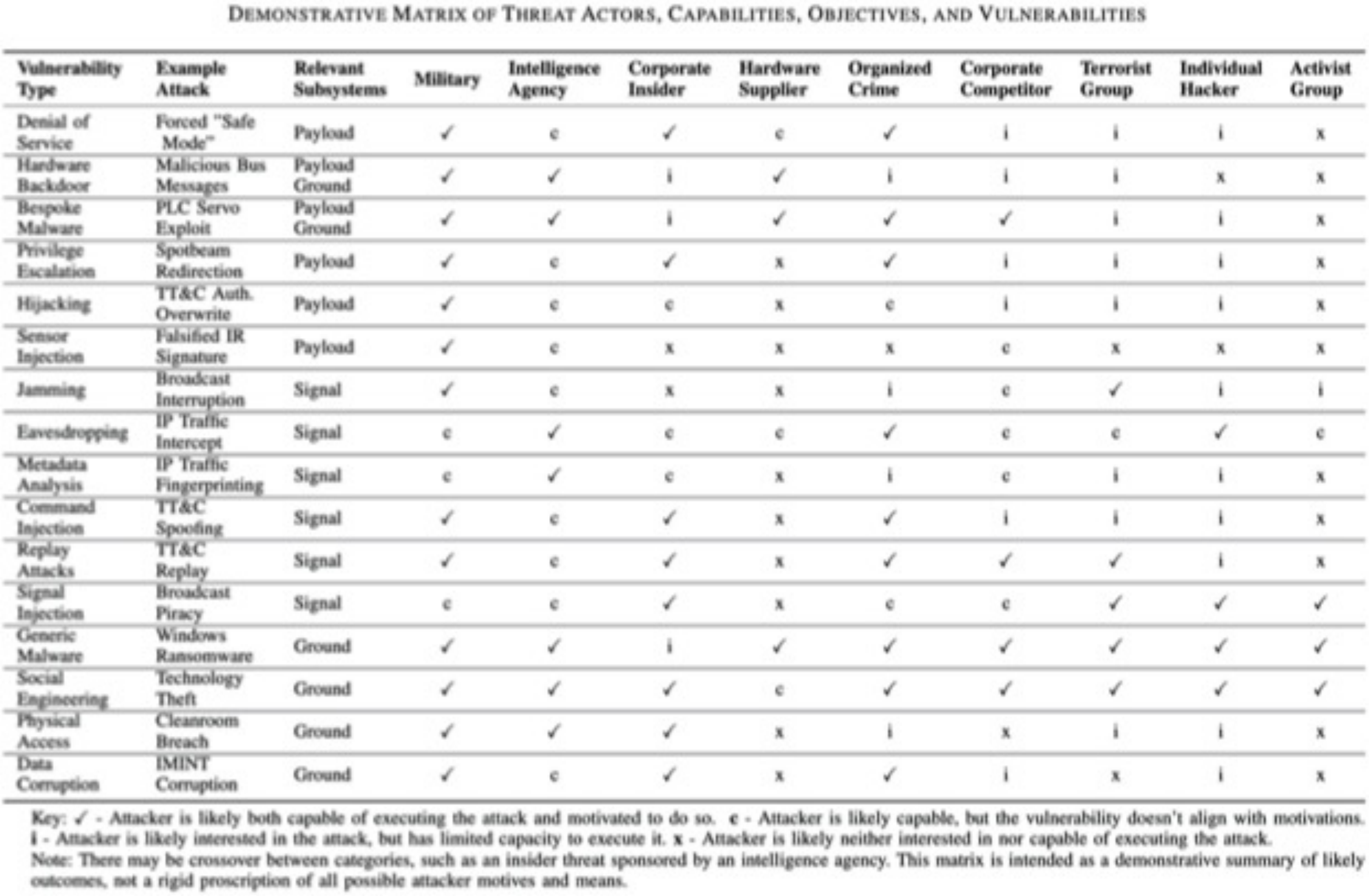
Image: https://www.nasa.gov/sites/default/files/thumbnails/image/fig_12.2_ground_system_architecture.png

Counterspace Continuum



Source: Defense Intelligence Agency; *Challenges to Security in Space,* February 11, 2019, pages 9, 20, 29, and 36, https://www.dia.mil/Portals/27/Documents/News/ Military%20Power%20Publications/Space_Threat _V14_020119_sm.pdf

Space Threat Actors



Demonstrative Matrix of Threat Actors, Capabilities, Objectives, and Vulnerabilities

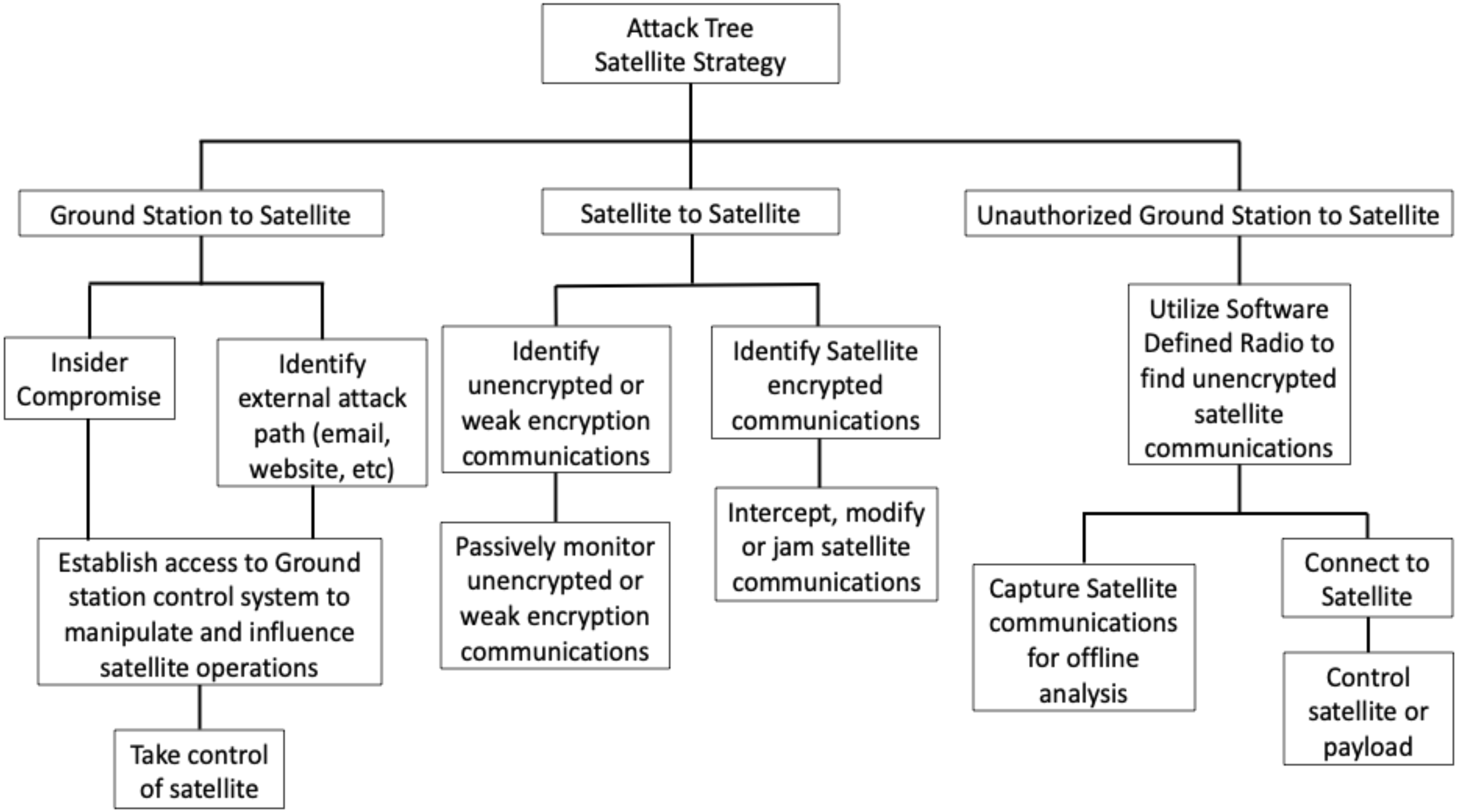
Vulnerability Type	Example Attack	Relevant Subsystems	Military	Intelligence Agency	Corporate Insider	Hardware Supplier	Organized Crime	Corporate Competitor	Terrorist Group	Individual Hacker	Activist Group
Denial of Service	Forced "Safe Mode"	Payload	✓	c	✓	c	✓	i	i	i	x
Hardware Backdoor	Malicious Bus Messages	Payload Ground	✓	✓	i	✓	i	i	i	x	x
Bespoke Malware	PLC Servo Exploit	Payload Ground	✓	✓	i	✓	✓	✓	i	i	x
Privilege Escalation	Spotbeam Redirection	Payload	✓	c	✓	x	✓	i	i	i	x
Hijacking	TT&C Auth. Overwrite	Payload	✓	c	c	x	c	i	i	i	x
Sensor Injection	Falsified IR Signature	Payload	✓	c	x	x	x	c	x	x	x
Jamming	Broadcast Interruption	Signal	✓	c	x	x	i	c	✓	i	i
Eavesdropping	IP Traffic Intercept	Signal	c	✓	c	c	✓	c	c	✓	c
Metadata Analysis	IP Traffic Fingerprinting	Signal	c	✓	c	x	i	c	i	i	x
Command Injection	TT&C Spoofing	Signal	✓	c	✓	x	✓	i	i	i	x
Replay Attacks	TT&C Replay	Signal	✓	c	✓	x	✓	✓	✓	i	x
Signal Injection	Broadcast Piracy	Signal	c	c	✓	x	c	c	✓	✓	✓
Generic Malware	Windows Ransomware	Ground	✓	✓	i	✓	✓	✓	✓	✓	✓
Social Engineering	Technology Theft	Ground	✓	✓	✓	c	✓	✓	✓	✓	✓
Physical Access	Cleanroom Breach	Ground	✓	✓	✓	x	i	x	i	i	x
Data Corruption	IMINT Corruption	Ground	✓	c	✓	x	✓	i	x	i	x

Key: ✓ - Attacker is likely both capable of executing the attack and motivated to do so. **c** - Attacker is likely capable, but the vulnerability doesn't align with motivations. **i** - Attacker is likely interested in the attack, but has limited capacity to execute it. **x** - Attacker is likely neither interested in nor capable of executing the attack.

Note: There may be crossover between categories, such as an insider threat sponsored by an intelligence agency. This matrix is intended as a demonstrative summary of likely outcomes, not a rigid proscription of all possible attacker motives and means.

Source: https://arxiv.org/pdf/2010.10872.pdf

Satellite Attack Strategy



Attack Tree Satellite Strategy

Ground Station to Satellite

- Insider Compromise
- Identify external attack path (email, website, etc)
- Establish access to Ground station control system to manipulate and influence satellite operations
- Take control of satellite

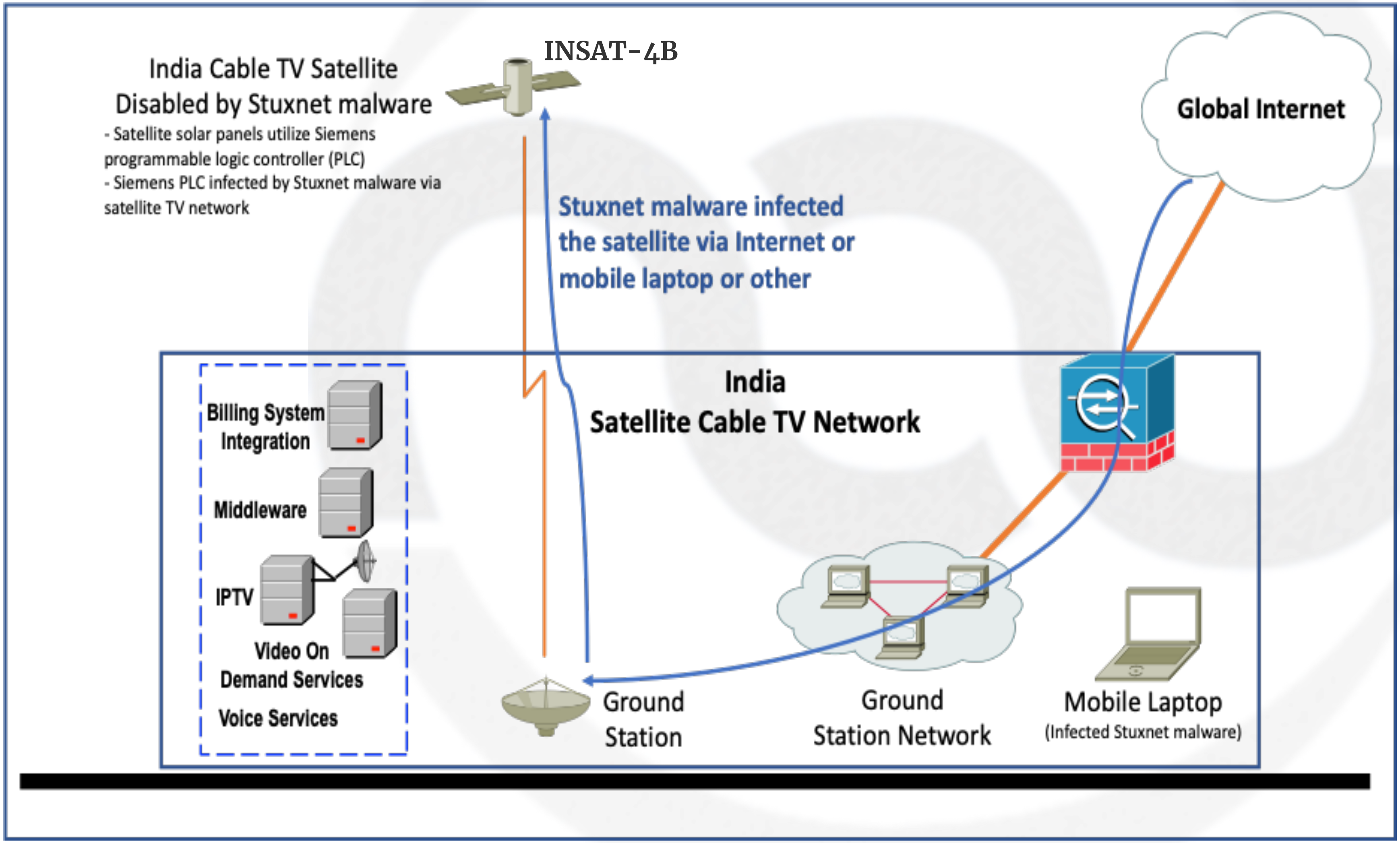
Satellite to Satellite

- Identify unencrypted or weak encryption communications
  - Passively monitor unencrypted or weak encryption communications
- Identify Satellite encrypted communications
  - Intercept, modify or jam satellite communications

Unauthorized Ground Station to Satellite

- Utilize Software Defined Radio to find unencrypted satellite communications
  - Capture Satellite communications for offline analysis
  - Connect to Satellite
    - Control satellite or payload

Did Malware Take Out the INSAT-4B Satellite?



India Cable TV Satellite Disabled by Stuxnet malware

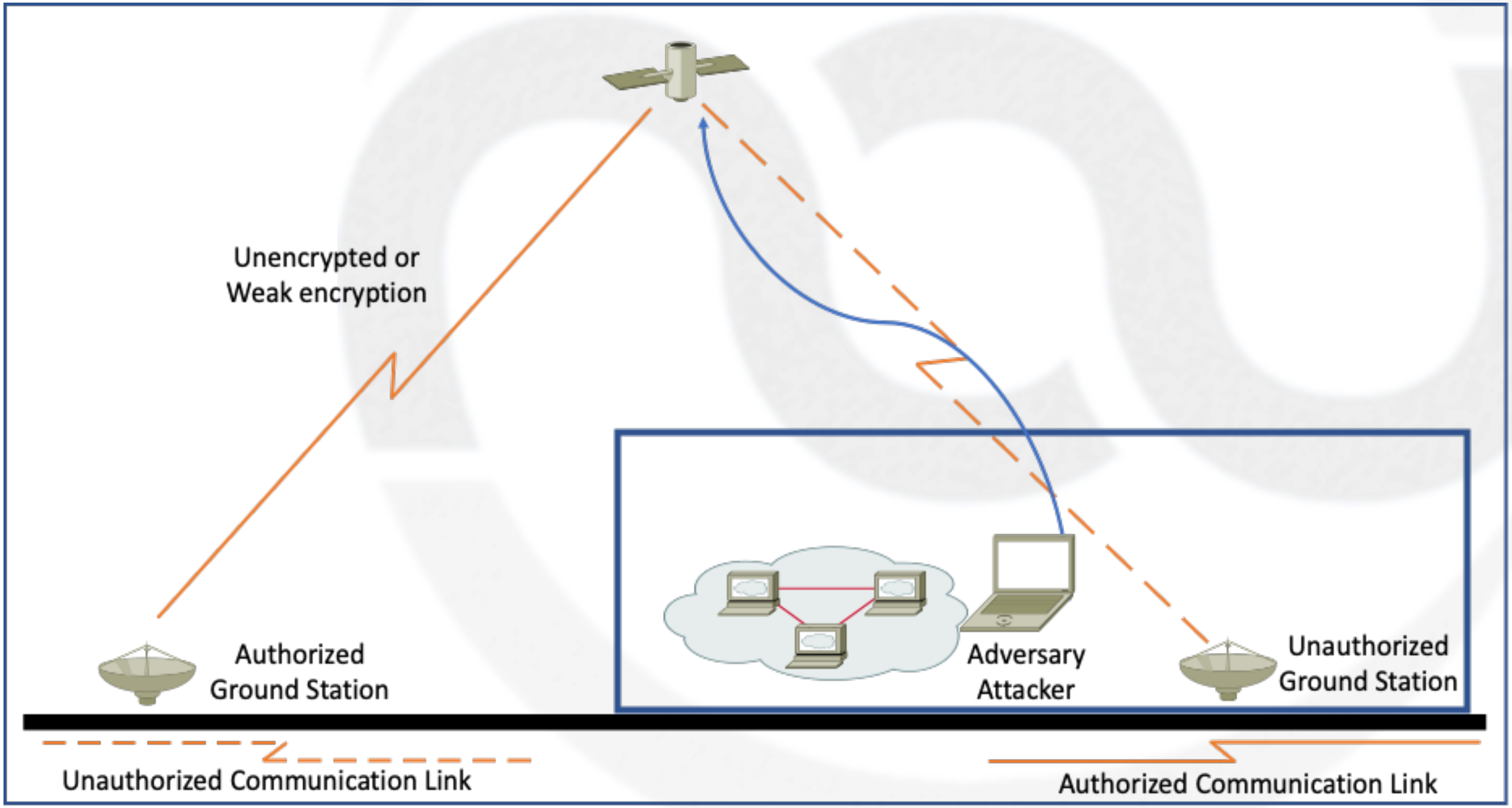
- Satellite solar panels utilize Siemens programmable logic controller (PLC)
- Siemens PLC infected by Stuxnet malware via satellite TV network

INSAT-4B
Stuxnet malware infected the satellite via Internet or mobile laptop or other
Global Internet
India
Satellite Cable TV Network
Billing System Integration
Middleware
IPTV
Video On Demand Services
Voice Services
Ground Station
Ground Station Network
Mobile Laptop
(Infected Stuxnet malware)

Source: https://www.forbes.com/sites/firewall/2010/09/29/did-the-stuxnet-worm-kill-indias-insat-4b-satellite/?sh=74a8a4b7127d

Unencrypted Satellite Communications

“ Radiation is one of the reasons information between Earth and many spacecraft is exchanged without encryption. Should radiation damage the storage area used for the encryption key, communication will be disrupted.” Igor Kuksov 9/13/2019



Source: https://usa.kaspersky.com/blog/internet-in-space/18618/
Reference: https://www.esa.int/ESA_Multimedia/Images/2019/07/Cryptography_ICE_Cube_experiment

Unencrypted Satellite Communications

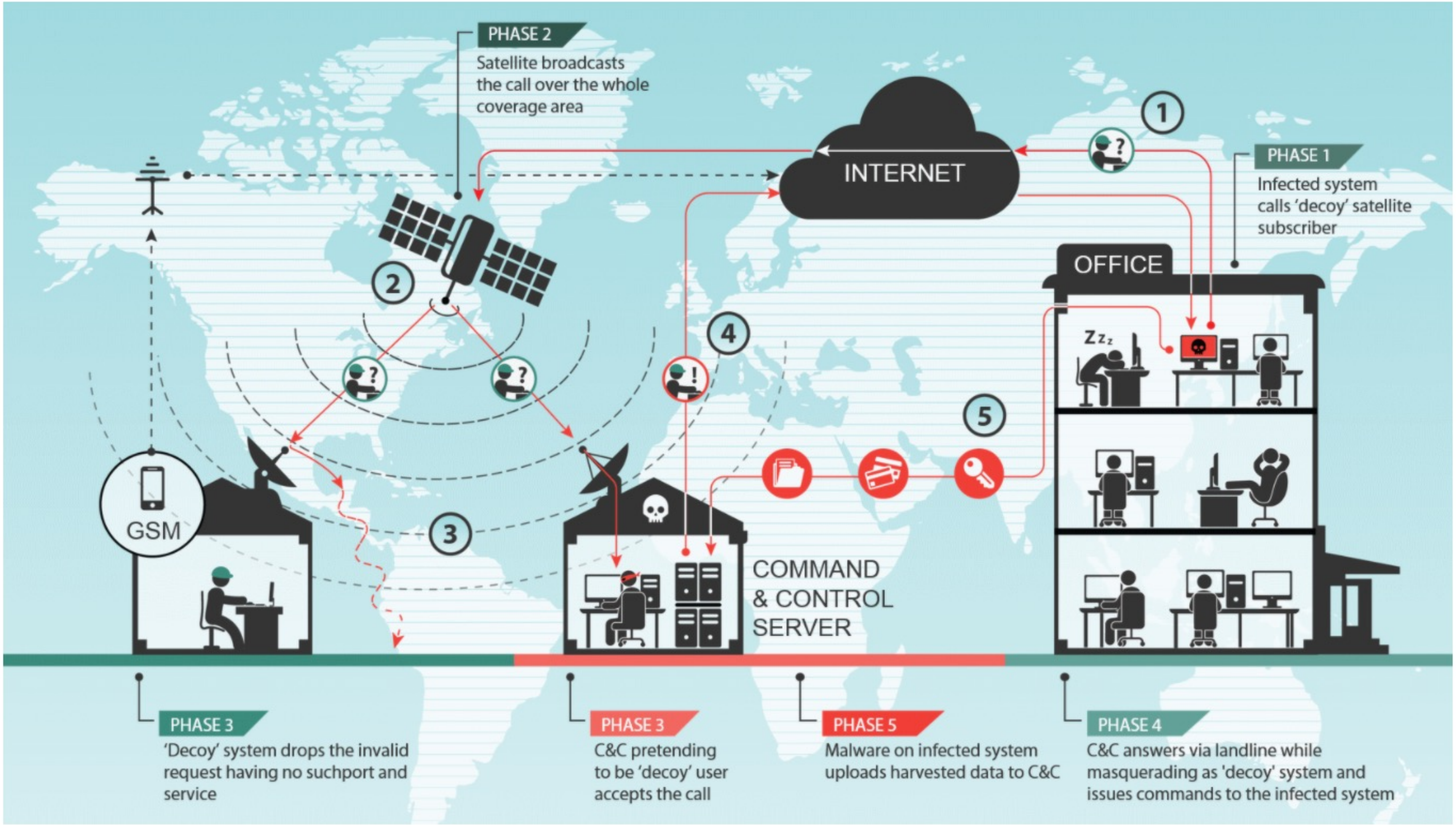
Enables Unauthorized CB Radio Communications

- Brazilian satellite hackers use high-performance antennas and homebrew gear to turn U.S. Navy satellites into their personal CB radios. Photo: Divulgação/Polícia Federal CAMPINAS, Brazil — On the night of March 8, cruising 22,000 miles above the Earth, U.S. Navy communications satellite FLTSAT-8 suddenly erupted with illicit activity. Jubilant voices and anthems crowded the channel on a […]
- 39 arrested across 6 Brazilian states
- "This had been happening for more than five years," says Celso Campos, of the Brazilian Federal Police. "Since the communication channel was open, not encrypted, lots of people used it to talk to each other."

Source: https://www.wired.com/2009/04/fleetcom/?currentPage=all

Unencrypted Satellite Communications Exploited by Turla Malware for C2

nousystems inc


PHASE 2
Satellite broadcasts the call over the whole coverage area
INTERNET
1
PHASE 1
Infected system calls 'decoy' satellite subscriber
OFFICE
2
4
Zzz
5
GSM
3
COMMAND & CONTROL SERVER
PHASE 3
'Decoy' system drops the invalid request having no suchport and service
PHASE 3
C&C pretending to be 'decoy' user accepts the call
PHASE 5
Malware on infected system uploads harvested data to C&C
PHASE 4
C&C answers via landline while masquerading as 'decoy' system and issues commands to the infected system

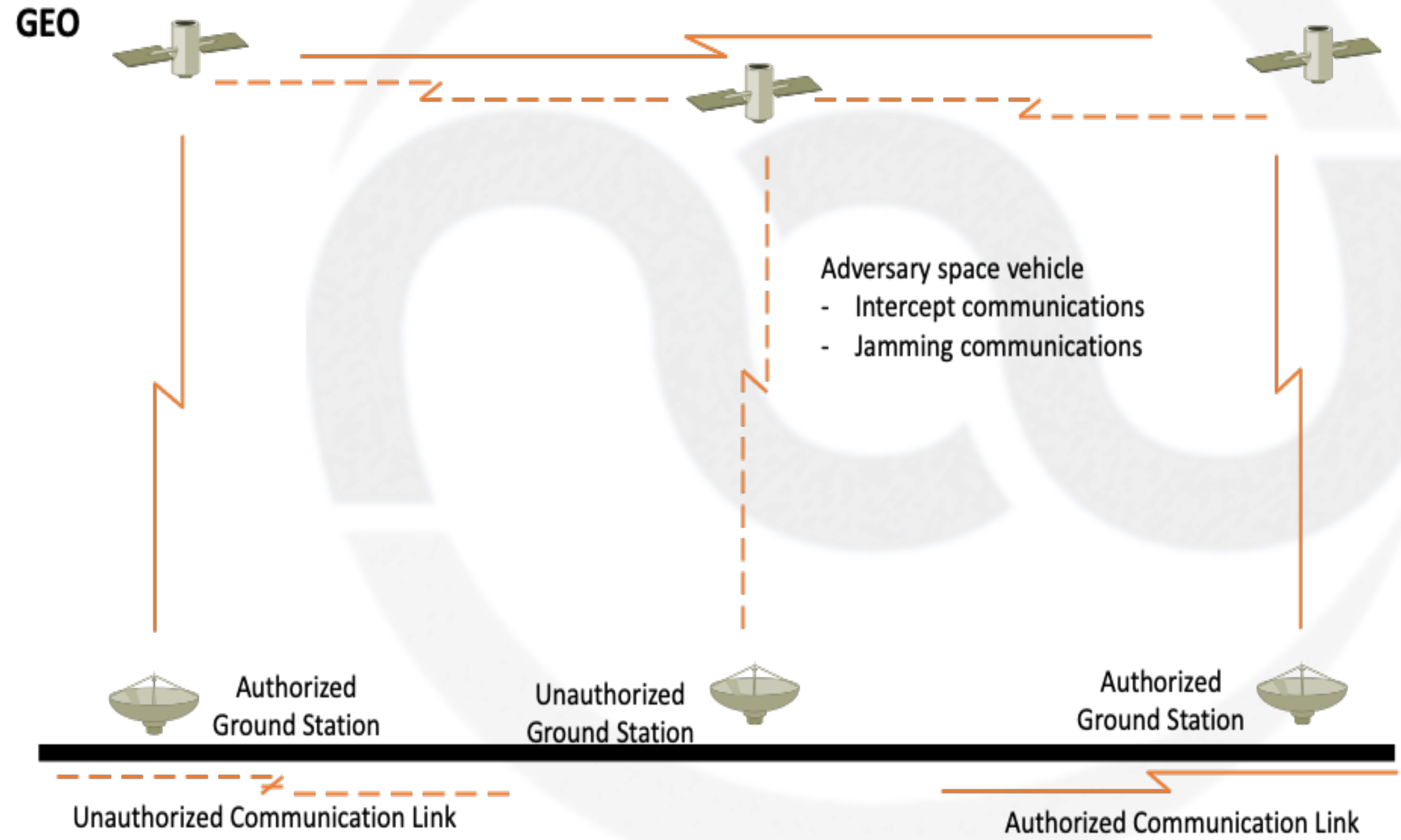
Source: https://media.kaspersky.com/pdf/SatTurla_Solution_Paper.pdf

Unencrypted Satellite Communications

- In 2009, it was revealed that insurgents in Iraq were using commercially available software to intercept and decode video over satellite communication links from U.S. surveillance aircraft. This was possible because some U.S. aircraft did not have the equipment needed to encrypt video feeds, and it enabled the insurgents to see what the U.S. military was seeing in near real-time.

Source: Richard B. Langley, “Innovation: GNSS Spoofing Detection,” GPS World, June 1, 2013, http://gpsworld.com/innovation-gnss-spoofing-detection-correlating-carrier-phase-with-rapid-antenna-motion/.

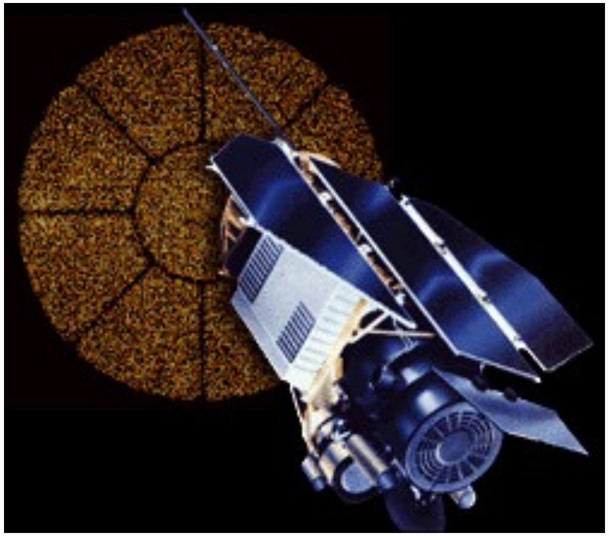
RF or Optical link interception (Theoretical)

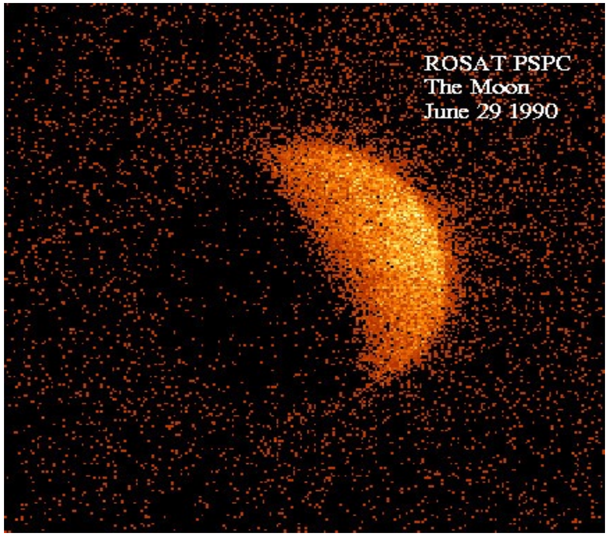

GEO
Adversary space vehicle
- Intercept communications
- Jamming communications
Authorized Ground Station
Unauthorized Ground Station
Authorized Ground Station
Unauthorized Communication Link
Authorized Communication Link

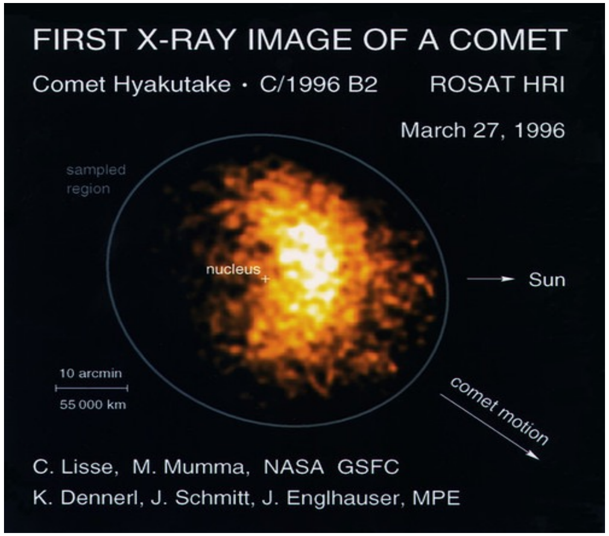
Source: https://www.hdi-specialty.com/downloads/_Global/HDIS209_Satellite%20Cyberattack_whitepaper_V8_05JULY21.pdf

ROSAT

1998 A US-German ROSAT satellite, used for peering into deep space, was rendered useless after it turned suddenly toward the sun damaging the High Resolution Imager by exposure. NASA investigators later determined that the accident was linked to a cyber-intrusion at the Goddard Space Flight Center. The attack allegedly originated from Russia (Epstein and Elgin 2008).






FIRST X-RAY IMAGE OF A COMET
Comet Hyakutake • C/1996 B2
ROSAT HRI
March 27, 1996
sampled region
nucleus
Sun
10 arcmin
55 000 km
comet motion
C. Lisse, M. Mumma, NASA GSFC
K. Dennerl, J. Schmitt, J. Englhauser, MPE

Source: https://cm.scholasticahq.com/article/5906-satellite-hacking-a-guide-for-the-perplexed
Images: https://asd.gsfc.nasa.gov/blueshift/index.php/2011/10/17/blog-a-fond-farewell-to-rosat/

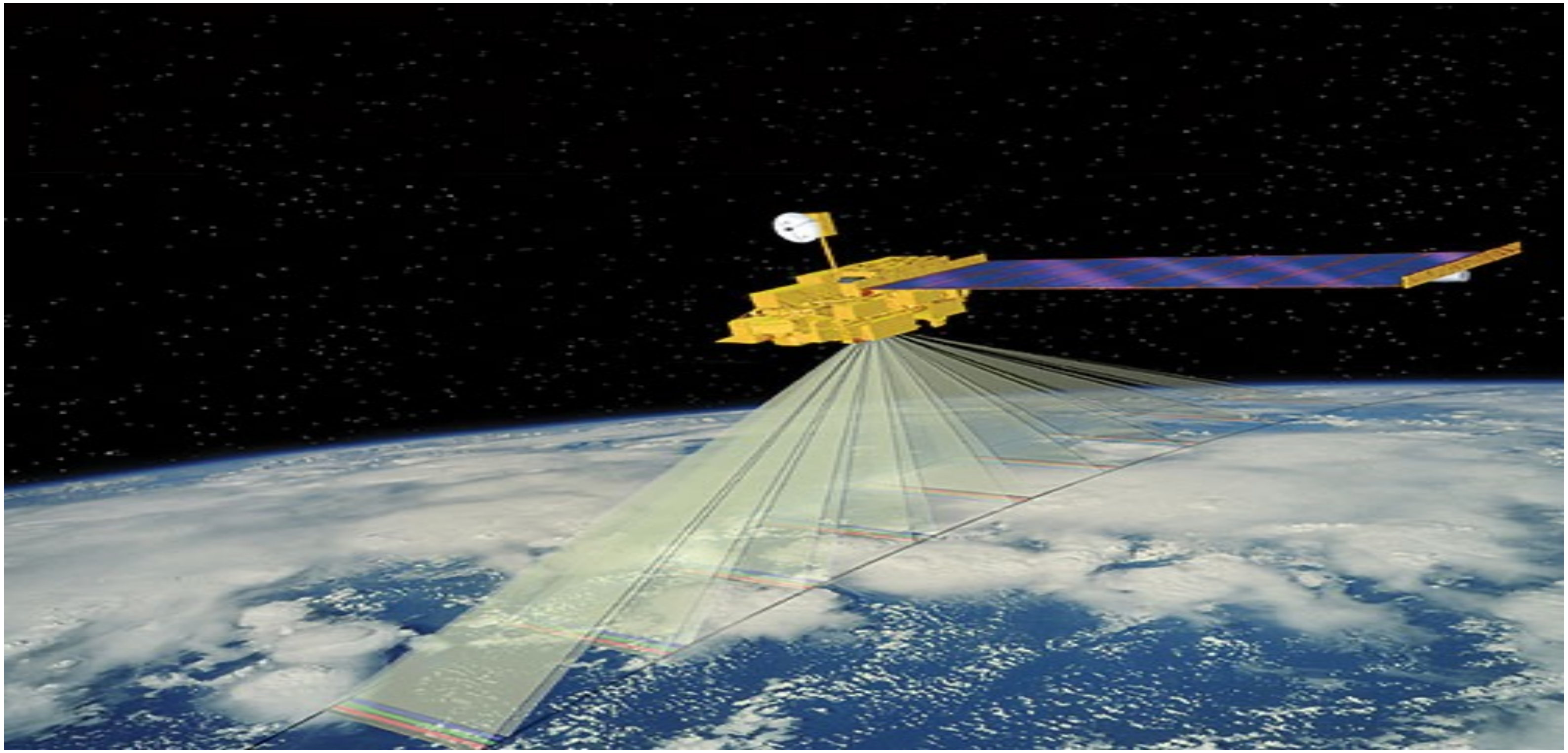
Landsat 7 satellite

12 minutes of "interference" in October 2007 and July 2008

Source: https://www.theguardian.com/technology/2011/oct/27/chinese-hacking-us-satellites-suspected
Images: https://landsat.gsfc.nasa.gov/article/successful-maneuver-spells-beginning-end-landsat-7

Terra satellite

2 minutes of "interference" in June 2008 and 9 minutes in October 2008



Source: https://www.theguardian.com/technology/2011/oct/27/chinese-hacking-us-satellites-suspected
Images: https://eospso.nasa.gov/missions/terra

NOAA Weather Satellites

nousystems inc

Chinese hack U.S. weather systems, satellite network - 2014

Source: https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html
Image: NOAA

UK Skynet Satellite

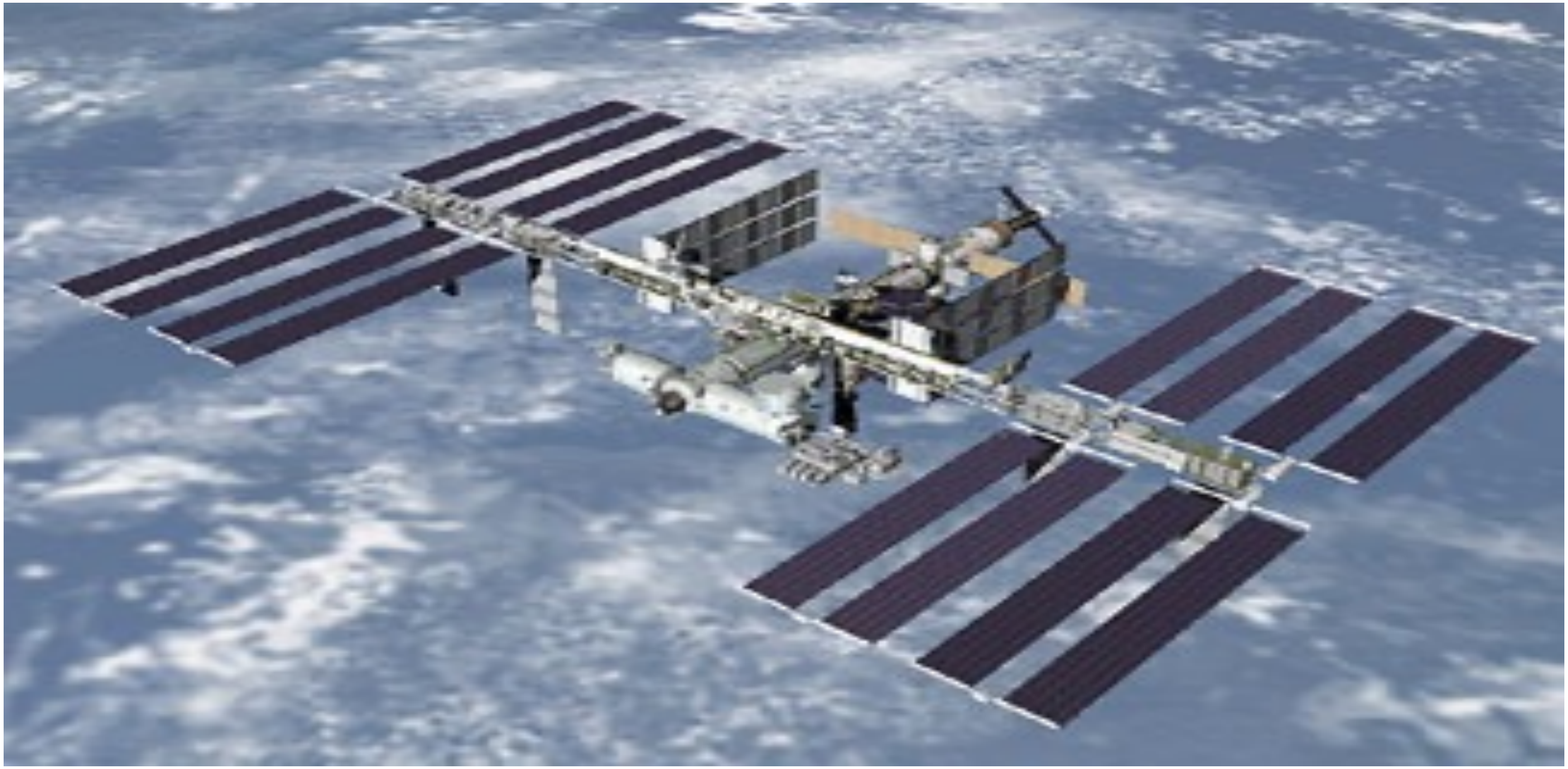
Satellite Hacked and Held for Ransom by Hackers - 1999

Source: http://content.time.com/time/magazine/article/0,9171,20673,00.html
Image: https://www.airbus.com/space/united-kingdom.html

Russia USB Drive & Laptop Infected ISS Prior to 2013

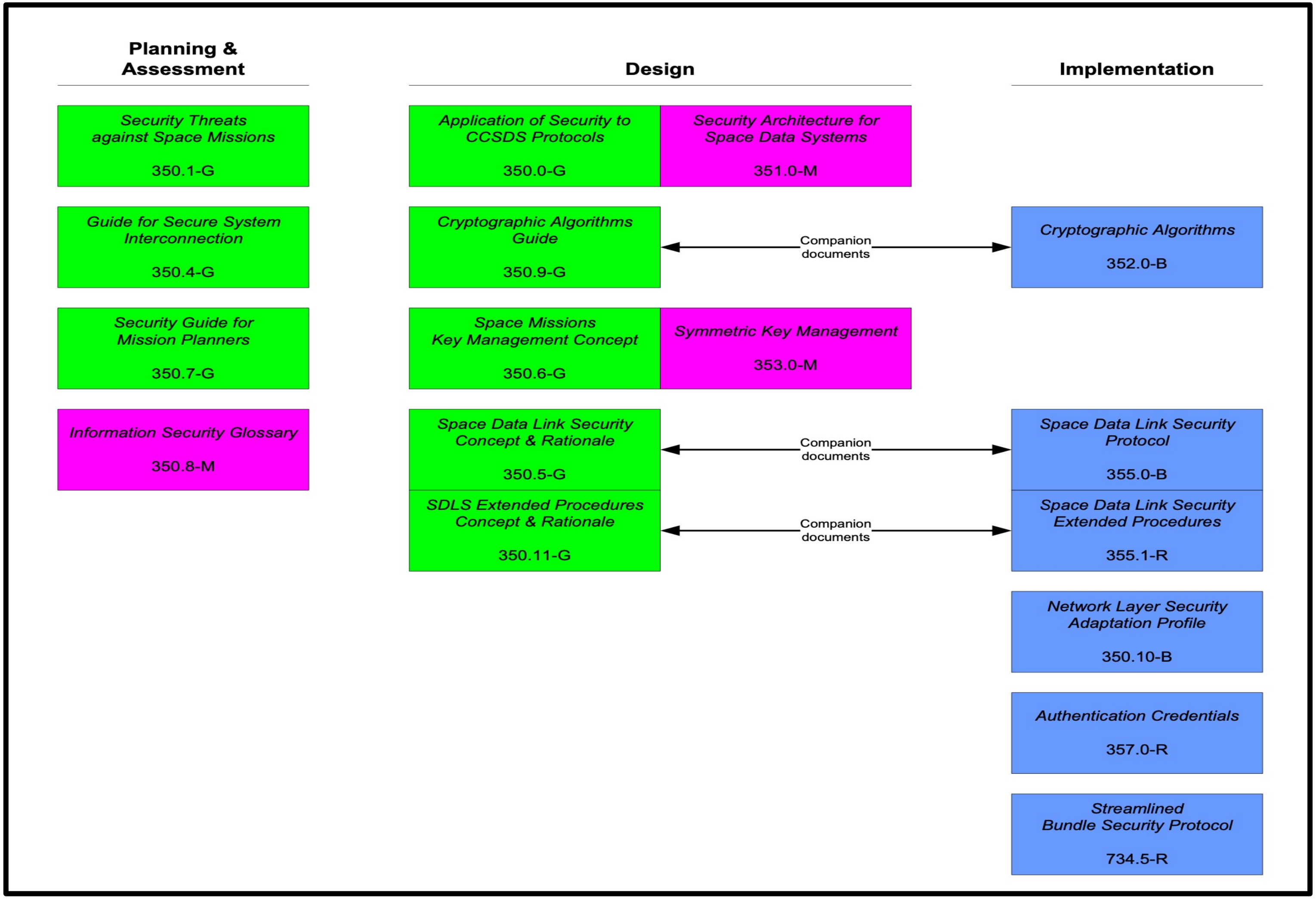
nousystems inc

- Russian astronaut infected International Space Station with a USB Flash drive containing malware
- Russian astronaut with Infected Windows XP laptop was brought onto the ISS infecting other Windows systems on network with W32.Gammima.AG worm



Source - http://www.usbtips.com/international-space-station-infected-with-usb-flash-drive-malware-carried-on-board-by-russian-astronauts/
Image - https://www.nasa.gov/mission_pages/station/main/iss_construction.html

Consultative Committee for Space Data Systems (CCSDS) Security Documents



Planning & Assessment

Security Threats against Space Missions 350.1-G

Guide for Secure System Interconnection 350.4-G

Security Guide for Mission Planners 350.7-G

Information Security Glossary 350.8-M

Design

Application of Security to CCSDS Protocols 350.0-G

Security Architecture for Space Data Systems 351.0-M

Cryptographic Algorithms Guide 350.9-G

Space Missions Key Management Concept 350.6-G

Symmetric Key Management 353.0-M

Space Data Link Security Concept & Rationale 350.5-G

SDLS Extended Procedures Concept & Rationale 350.11-G

Implementation

Cryptographic Algorithms 352.0-B

Space Data Link Security Protocol 355.0-B

Space Data Link Security Extended Procedures 355.1-R

Network Layer Security Adaptation Profile 350.10-B

Authentication Credentials 357.0-R

Streamlined Bundle Security Protocol 734.5-R

Source: The Consultative Committee for Space Data Systems, SECURITY GUIDE FOR MISSION PLANNERS, https://public.ccsds.org/Pubs/350x7g2.pdf

Space Cybersecurtiy Best Practices, Guidelines and Policies

Organization	Title	Link
Mitre	CYBER BEST PRACTICES FOR SMALL SATELLITES	https://www.mitre.org/publications/technical-papers/cyber-best-practices-for-small-satellites
National Institute of Standards and Technology (NIST)	Introduction to Cybersecurity for Commercial Satellite Operations	https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8270-draft.pdf
Committee on National Security Systems (CNSS)	NATIONAL INFORMATION ASSURANCE INSTRUCTION FOR SPACE SYSTEMS USED TO SUPPORT NATIONAL SECURITY MISSIONS	https://www.cnss.gov/CNSS/issuances/Instructions.cfm
Committee on National Security Systems (CNSS)	SECURITY CATEGORIZATION AND CONTROL SELECTION FOR NATIONAL SECURITY SYSTEMS	https://www.cnss.gov/CNSS/issuances/Instructions.cfm
Committee on National Security Systems (CNSS)	Space Platform Overlay	https://www.cnss.gov/CNSS/issuances/Instructions.cfm
Committee on National Security Systems (CNSS)	CYBERSECURITY POLICY FOR SPACE SYSTEMS USED TO SUPPORT NATIONAL SECURITY MISSIONS	https://www.cnss.gov/CNSS/issuances/Policies.cfm
National Institute of Standards and Technology (NIST)	Cybersecurity Framework	https://www.nist.gov/cyberframework
Aerospace Corporation	ESTABLISHING SPACE CYBERSECURITY POLICY, STANDARDS, AND RISK MANAGEMENT PRACTICES	https://aerospace.org/sites/default/files/2020-10/Bailey%20SPD5_20201010%20V2_formatted.pdf
Executive Office of the President	Space Policy Directive-5 Cybersecurity Principles for Space Systems	https://www.federalregister.gov/documents/2020/09/10/2020-20150/cybersecurity-principles-for-space-systems
The Consultative Committee for Space Data Systems (CSDS)	SECURITY GUIDE FOR MISSION PLANNERS	https://public.ccsds.org/Pubs/350x7g2.pdf
Orbital Security Alliance	Commercial Space System Security Guidelines	https://www.orbitalsecurity.space/pubs
National Oceanic and Atomospheric Administration (NOAA)	Licensing of Private Remote Sensing Space Systems	https://www.federalregister.gov/documents/2020/05/20/2020-10703/licensing-of-private-remote-sensing-space-systems

Secure the Spacecraft

- DevSecOps
- Supply Chain
- Zero Trust
- Defense in Depth
- Encryption
- Logging
- Intrusion Prevent System
- Machine Learning and Artificial Intelligence
- TT&C monitoring
- System Configuration Management

Thanks to NANOG team!

Questions?

@PaulCoggin